

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

(19)

JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **06236325 A**

(43) Date of publication of application: **23.08.94**

(51) Int. Cl

G06F 12/14
G11C 16/06

(21) Application number: **05020155**

(71) Applicant: **SANSEI DENSHI JAPAN KK**

(22) Date of filing: **08.02.93**

(72) Inventor: **AMASHIRO JIYUNYA**

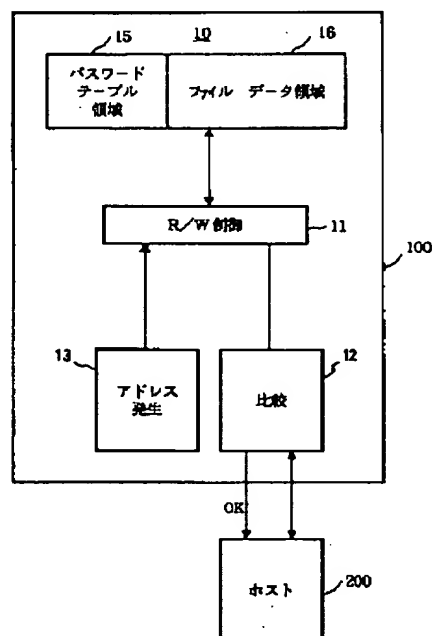
(54) **DATA STORAGE DEVICE**

(57) Abstract:

PURPOSE: To provide the data storage device which can surely protect stored information.

CONSTITUTION: The data storage device which reads stored data in response to access from an external device 200 has a password storage area 10 in which password information is written and a comparing circuit 12 which compares a password sent from the external device with a password read out of the password storage area and allows the external device to read specified data out when both the passwords match each other.

COPYRIGHT: (C)1994,JPO&Japio



(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号

特開平6-236325

(43)公開日 平成6年(1994)8月23日

(51)Int.Cl.⁴

G 0 6 F 12/14

G 1 1 C 18/08

識別記号

3 2 0 C 9293-5B

6866-5L

庁内整理番号

F I

G 1 1 C 17/ 00

技術表示箇所

3 0 9 F

審査請求 未請求 請求項の数3 OL (全 5 頁)

(21)出願番号 特願平5-20155

(22)出願日 平成5年(1993)2月8日

(71)出願人 591021763

三星電子ジャパン株式会社

東京都中央区日本橋浜町2丁目31番1号

(72)発明者 天白 順也

東京都千代田区神田須田町2-3 三星電
子ジャパン株式会社内

(74)代理人 弁理士 大塚 康徳 (外1名)

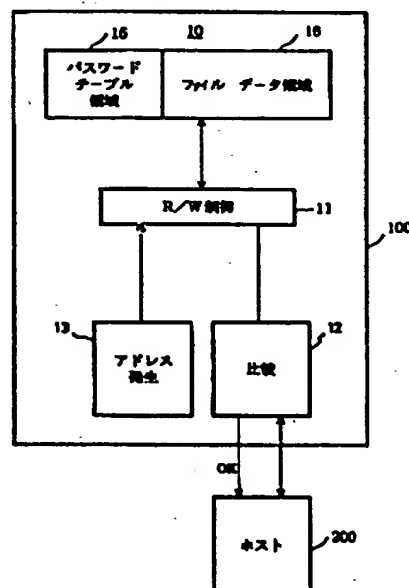
(54)【発明の名称】 データ記憶装置

(57)【要約】

【目的】 記憶された情報を確実に保護することのできるデータ記憶装置を提供することを目的とする。

【構成】 外部の装置200からのアクセスに応じて記憶したデータを読み出すデータ記憶装置において、パスワード情報を書き込むためのパスワード記憶領域10と、前記外部の装置から送られてきたパスワードと前記パスワード記憶領域から読み出したパスワードとを比較する比較回路12とを有し、比較が一致したときに、指定されたデータを前記外部の装置が読み取ることを許可する。

第 1 図



【特許請求の範囲】

【請求項1】 外部の装置からのアクセスに応じて記憶したデータを読み出すデータ記憶装置において、記憶媒体上に設けられ、パスワード情報を書き込むためのパスワード記憶領域と、

前記外部の装置から送られてきたパスワードと前記パスワード記憶領域から読み出したパスワードとを比較する比較手段とを有し、

前記比較手段による比較が一致したときに、アクセス対象の記憶されたデータを前記外部の装置がアクセスすることを許可する手段とを備えることを特徴とするデータ記憶装置。

【請求項2】 請求項1のデータ記憶装置において、前記パスワード記憶領域は前記記憶媒体上の異なる部分に夫々設けられ、前記比較手段は、前記複数の記憶領域から読み出した複数のパスワードのなかでもっとも多く一致するデータ内容と前記外部の装置から送られてきたパスワードとを比較することを特徴とするデータ記憶装置。

【請求項3】 請求項2のデータ記憶装置において、前記記憶媒体は、

フラッシュEEPROMで構成されるとともに、個々のパスワードを記憶するこの記憶媒体上の番地を表すポインタデータを記憶するポインタ記憶領域と、前記ポインタデータとリンクされ、実際のパスワードデータを記憶する領域とを有することを特徴とするデータ記憶装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、データ記憶装置に関し、特に、データ記憶装置に記憶されたデータの機密保護の改良に関する。

【0002】

【従来の技術】 記憶媒体に記憶された情報データには色々な保護が行なわれている。代表的な保護の手法は、ハード的な又はソフト的なライトプロテクション(Write Protection)である。ハード的なライトプロテクションは書き込み保護の爪であり、ソフト的なライトプロテクションとは、記録媒体のファイル毎に、アクセスを許可するか(更に、データの変更を許可するか)の情報をディレクトリに加えると言うものである。

【0003】

【発明が解決しようとする課題】 しかし上述のライトプロテクションは、あくまでも注意若しくは警告程度の機能しか有さず、任意の(第三者による)データの読み出しに対してライトプロテクション機能は働かない。プログラミング言語では、データファイルにオーナー指定ができ、パスワードを知らない本人以外には読み出せなくするモードがあるが、この機能もスーパーユーザ等の特権パスワードを有するものに読み出されてしまうという問題

がある。

【0004】 本発明は、前記従来の欠点を除去するために提案されたもので、記憶された情報を確実に保護することのできるデータ記憶装置を提供することを目的とする。

【0005】

【課題を解決するための手段】 この課題を解決するため、本発明のデータ記憶装置は、外部の装置からのアクセスに応じて記憶したデータを読み出すデータ記憶装置において、記憶媒体上に設けられ、パスワード情報を書き込むためのパスワード記憶領域と、前記外部の装置から送られてきたパスワードと前記パスワード記憶領域から読み出したパスワードとを比較する比較手段とを有し、前記比較手段による比較が一致したときに、アクセス対象の記憶されたデータを前記外部の装置がアクセスすることを許可する手段とを備えることを特徴とする。

【0006】

【実施例】 以下、添付図面を参照しながら本発明の好適な実施例を説明する。この実施例では、記憶媒体として、通常ファイルデータと更にまたパスワードデータをも記憶するフラッシュEEPROMを使用する。そこで、この実施例では、とくに断らないかぎり、フラッシュEEPROMを簡単に「メモリ」と称する。

【0007】 図1は、本実施例のデータ記憶装置100の構成図である。記憶装置100はデータ及びパスワードを記憶するためのメモリ10を有する。200は、記憶装置100と通信することにより、記憶装置100のメモリ10上のデータ及びパスワードをアクセスする例えばパソコン等のホストコンピュータである。データ記憶装置100は、メモリ10と、このメモリ10へのデータの読み出し/書き込みを制御する制御回路11と、アドレスを発生するアドレス発生器13とを有する。メモリ10は、図示するように、パスワードの記憶番地を記憶する領域(パスワードテーブル15)と、通常データ(ファイルデータ)を記憶する領域16とを有する。アドレス発生器13は、パスワードテーブル15から読み取ったアドレスからメモリ10上の実際のパスワード格納アドレスを発生する。発生器13が発生したアドレスに従って、制御回路11はメモリ10の領域16からパスワードデータを読み出す。また更に、記憶装置100は、制御回路11が読み出したパスワードとホスト200から送られてきたパスワードとを比較し、比較で一致が取れば、ホスト200に対してアクセスが許される意味の信号OKを送る。

【0008】 図2は、ホスト200と記憶装置100との間での、データの読み出し書き込みに関するインタフェース信号を示す。ホスト200からは、読み出しを要求する信号RD/(／は反転信号を表す)又は書き込みを要求する信号WT/が送られてくる。これらの要求信号は、前述の信号OKが真の時のみ、読み出し若しく

3

は書き込みを許可する信号RDX、WDXとなる。一方、信号OKはホスト200にも送られる。即ち、ホスト200はアクセスが許可されたか否かを、信号OKをモニタすることにより分かる。また、ディスク装置100側では、信号信号RDX、WTXが真にならないかぎり、実際の読み出し、書き込みは禁止される。

【0009】図3は、パスワードテーブル15に記憶されたパスワードアドレスと、メモリ10上のアドレスとの関係を示す。周知のように、フラッシュメモリ10は、複数のブロック単位でアクセスが可能である。そこで、この実施例では、ブロック毎にパスワードを1つつ記憶する。本実施例では、5個（拡張は可能である）までのパスワードの記憶を許す。従って、パスワードテーブル15は5つのエントリを有する。図3の例では、#1～#5までのエントリが設定されている。各エントリの番地は固定である。各エントリの最初のフィールドは、そのパスワードが使用されているか否かを示すビットである。そのビットが1であれば、そのパスワードは使われており、0であれば使用されていないことを示す。使用／不使用を示すビットの次のフィールドは、そのパスワードが記憶されているメモリ10上のアドレスである。使用／不使用フィールドが1であるエントリから読みだされたアドレスデータはアドレス発生器13に渡されて、この発生器がパスワードを実際に記憶している絶対番地を発生して、制御回路11がそのパスワードデータを読み出す。

【0010】ところで、フラッシュEEPROMは耐久性の点で問題がある。そこで、記憶装置100の不図示のエラーチェック回路がメモリ10からの読み出しパスワードアドレスデータにエラーを検出したときには、対応するパスワードテーブル15のエントリ上に例えば“FFFF”を書き込んでおく。もし、メモリ10から読みだされたデータが“FFFF”ならば、そのパスワードは信頼が置けないことを意味する。また、当該エラーの発生したメモリ10上のアドレスにも“FFFF”を書き込んでおく。

【0011】図3に示すように、本実施例では、パスワードは5つまで設定できる。5つとしたのは、読み出された5つのパスワードに不一致が合った場合に、多数決方式によって決定するためである。図4は比較回路12と制御回路14との関係を示す。比較回路は、デジタルコンパレータ41と、インバータ42と、アップダウンカウンタ43とを有する。カウンタ43は、ホスト200から送られてきたパスワードとメモリ10から読み出したパスワード（RDデータ）との比較結果において、一致の回数と不一致の回数を相補的にカウントするものである。

【0012】計数に先立ち、ホスト200から新たなパスワードが送られてきたならば、制御回路14はカウンタ43に対してクリア信号CLRを送ってカウンタ43

をクリアする。コンパレータ41は、ホスト200から送られてきたパスワードとメモリ10から読み出したパスワード（RDデータ）とを比較する。一致信号は、カウンタ43のアップカウント端子（UP）に入力される。一致信号はインバータ42により反転されて、不一致信号としてダウンカウント端子（DN）に入力される。

【0013】記憶された全てのパスワードについて検索されたかいかは、制御回路14が使用／不使用フィールドが1であるか0であるかを見て判断する。全てのパスワードについて検索されたならば、制御回路14はカウンタ43の端子（OE）に対して、その出力を付勢する信号であるところの「終了」信号を送る。この信号が真になると、カウンタ43の出力端子（OUT）から信号OKが有効となる。

【0014】図3の例で、5つのパスワードが全て使用されていた場合において、ホストから送られてきたパスワードと、記憶されていたパスワードデータとが、3つについて一致し、2つについては不一致であったときには、カウンタ43は信号OKを出力する。本発明はその趣旨を逸脱しない範囲で種々変形が可能である。

【0015】例えば、前記実施例では、メモリ媒体にフラッシュメモリとしたが、本発明はそれ記憶媒体（例えば、ディスク装置等）にデータを記憶する装置にも適用可能である。また、上記実施例では、パスワードを記憶する記憶媒体（領域16）とパスワードアドレスを記憶する領域（パスワードテーブル15）とを同じものとしていた。しかし、本発明は、それらの記憶媒体が異なる装置に対しても適用可能である。

【0016】また、前記実施例では、パスワードデータをフラッシュメモリブロック毎に設定していたが、全てのパスワードデータ領域を1つのブロックに設定してもよい。また、上記実施例では、パスワードテーブルの開始番地は固定であるとした。これは、パスワードテーブルの開始番地をホスト側からアクセス不能にするためである。しかし本発明は、このパスワードテーブルの開始番地をホスト側のディレクトリ上にもたせてもよい。

【0017】

【発明の効果】以上説明したように本発明は、パスワード情報を書き込むためのパスワード記憶領域を備え、前記外部の装置から送られてきたパスワードと前記パスワード記憶領域から読み出したパスワードとを比較し、比較が一致したときに、アクセス対象の記憶されたデータを外部の装置がアクセスすることを許可するようにしたことにより、記憶された情報を確実に保護することのできるデータ記憶装置を提供することができる。

【図面の簡単な説明】

【図1】本実施例のデータ記憶装置100の基本的回路構成を示す図である。

【図2】データ記憶装置100とホスト200との間の

5

インタフェースを説明する図である。

【図3】記憶装置100におけるパスワードの記憶体系を説明する図。

【図4】比較回路の構成を示す図。

【符号の説明】

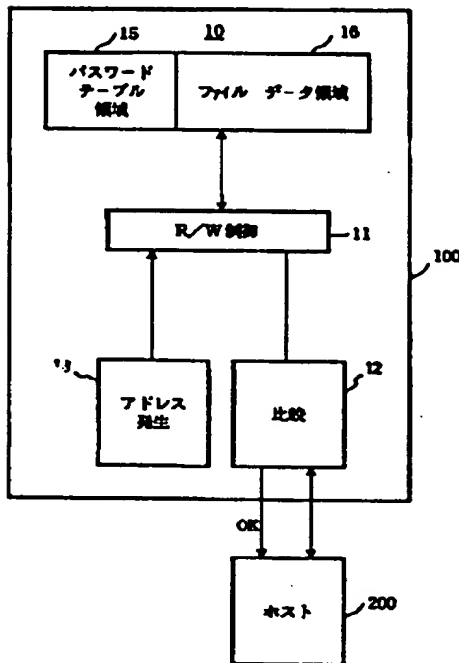
10…メモリ（フラッシュEEPROM）、11…R／

6

W制御回路、12…比較回路、13…アドレス発生器、14…R／W制御回路、15…パスワードテーブル、16…ファイルデータ領域、40、41…コンパレータ、43…UPダウンカウンタ、100…データ記憶装置、200…ホストコンピュータ

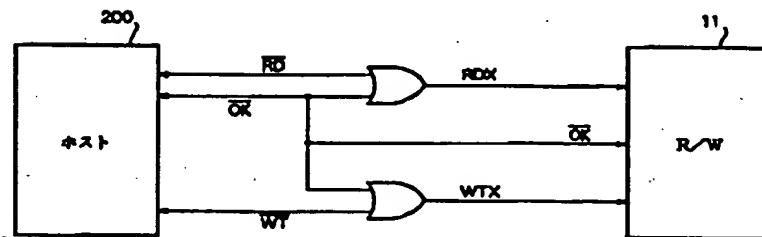
【図1】

第 1 図



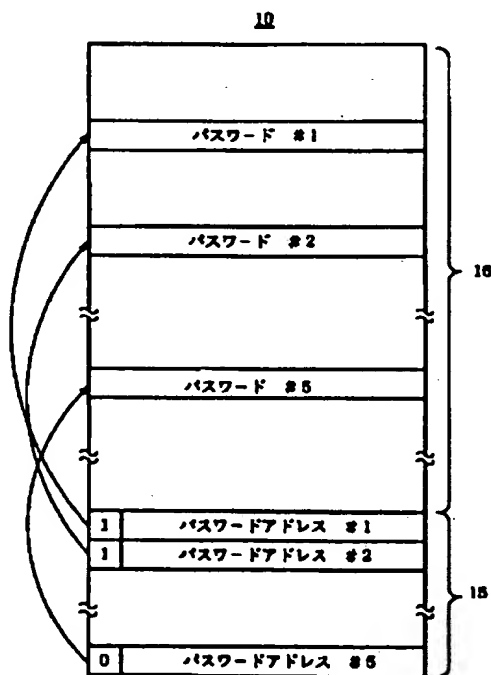
【図2】

第 2 図



【図3】

第 3 図



(5)

特開平6-236325

【図4】

